CHAPTER 9

Using WiMAX in Cisco Access Registrar

Revised: March 20, 2009, OL-17222-03

Cisco Access Registrar (CAR) 4.2 supports Worldwide Interoperability for Microwave Access (WiMAX) technology. This feature support in CAR 4.2 complies with the WiMAX forum NWG_R1.1.0_Stage-3 specifications.

WiMAX - An Overview

WiMAX is a standards-based wireless technology that offers high throughput broadband connections over long distances. WiMAX can be used for a number of applications, including “last mile” broadband connections, fixed and mobile cellular service, hotspots and cellular backhaul, and high-speed enterprise connectivity for business. WiMAX is based on the IEEE 802.16d standard for fixed wireless, and the 802.16e standard for mobile wireless. This standard is appealing to customers because it allows mass production of chipsets that reduce CPE costs, ensures multi-vendor interoperability, and reduces investment risk for operators.

The architectural framework of a WiMAX network consists of the Access Service Network (ASN), the Core Service Network (CSN), and a AAA server. An Access Service Network is a set of network functions that provide radio access to a WiMAX subscriber. The ASN typically provides functions such as network discovery and selection, connectivity service between the MSS and CSN, Radio Resource Management, Multicast and Broadcast Control, Intra-ASN mobility, Paging, and Location Management. The WiMAX architecture consists of both mobile and fixed subscribers, as well as the ASN and CSN.

A CSN is defined as a set of network functions that provide IP connectivity services to the WiMAX subscribers. CSN might comprise network elements such as Routers, Home Agent, AAA proxy/servers, user databases, Policy Servers, Content Service Gateways, Service Selection Gateways, and interworking gateway devices.

Figure 9-1 describes the network reference model of a typical WiMAX scenario.

Figure 9-1 WiMAX Network Reference Model

WiMAX in Cisco Access Registrar

CAR uses the Extensible Authentication Protocol (EAP) to enable the WiMAX feature. It also caches the IP attributes and Mobility Keys that are generated during network access authentication. To enable caching of the WiMAX attributes, you must configure the respective resource managers. See Configuring the Resource Manager for WiMAX, page 9-6, for information on configuring resource manager. Figure 9-2 shows the WiMAX workflow in CAR.

Figure 9-2 WiMAX Workflow

The WiMAX workflow in CAR includes:

- Direct interaction between the ASN GW and CAR
- Interaction between the ASN GW and CAR through the HA

Direct Interaction Between the ASN GW and Cisco Access Registrar

When the mobile node (MN) sends a RADIUS request to the ASN GW, it forwards this request to the CAR server initiating an authentication using the EAP service, **for example, eap-ttls**. The initial Access-Request containing the WiMAX capability and NAS-Port-Type (Type:61) attributes indicate that the specified flow is for a WiMAX request from ASN GW. CAR redirects this request to the WiMAX service that you configure. The WiMAX service redirects the request to the EAP-based Wimax-Authentication-Service for authentication. Upon successful authentication, the WiMAX service redirects the request to Wimax-Session-Manager to allocate the home agent. Subsequently, CAR generates the appropriate keys based on the Extended Master Session Key (EMSK) and records the generated keys in the session cache resource manager as configured, before sending Access-Accept to the ASN GW.

The authentication methods followed by CAR are:

- User-only
- Device-only
- Single-EAP Device or User authentication

Note CAR 4.2 does not support Double-EAP authentication.

CAR uses the following values to identify the service-type:

- Framed—for initial authentication
- Authenticate-Only—for reauthentication
- Authorize-Only—for prepaid request

Note Prepaid attributes can also be sent in the initial authentication.

The attributes contained in this flow are listed in Table 9-1. For detailed information on the attributes refer to the WiMAX forum NWG_R1.1.0_Stage-3 specifications document.

Table 9-1 Attributes: ASN GW-CAR Flow

Attribute	Description
User-Name	Must be present. This attributes gets the NAI from the EAP-Response/Identity.
Service-Type	Must be present and the value is Framed, Authenticate-Only or Authorize-Only.
WiMAX Capability	This attribute is chosen by the ASN GW. The request to the CAR is provided through the WiMAX-Capability attribute. The server might respond with the chosen WiMAX Capability.
NAS-Port-Type	The request must contain this attribute with the value 27. This indicates Wireless IEEE 802.16 port when coming from a WiMAX ASN.
Calling-Station-ID	The request must contain this attribute with the value set to the MAC address of the device in binary format.

Table 9-1 Attributes: ASN GW-CAR Flow (continued)

Attribute	Description
Device-Authentication-Indicator	The request might contain this attribute to indicate whether the device authentication was performed or not and the result of the action.
CUI	The NAS might intimate the support for CUI by sending the CUI attribute with the value 'null'.
GMT-Time-Zone-Offset	The request must contain the offsets in seconds from the GMT at the NAS.
Framed-IP-Address	This is the CMIPv4 Home address to be assigned to the MN. If this attribute is not present then the Home address is derived by the ASN from MIP procedures or through DHCP.
AAA-Session-ID	This attribute shall not be present in the initial authentication. The value is a unique identifier in the home realm for this session as set by the HAAA(CAR) in the Access-Accept, when the authentication is successful and it will be included in all subsequent requests from the NAS, such as online accounting.
MSK	The MSK shall be provided by the AAA server as a result of successful EAP-authentication. MSK can be transmitted using either the MS-MPPE-Keys or the MSK attribute.
Packet-Flow-Descriptor	The pre-provisioned service flow which might be present in the Access-Accept packet.
QoS-Descriptor	The pre-provisioned service flow which might be present in the Access-Accept packet, if configured in CAR.
BS-ID	Might be present in the Access-Request packet which will identify NAP-ID base station. If both NAP-ID and BS-ID are present, the NAP-ID will be ignored.
Acct-Interim-Interval	Sent in the Access-Accept packet. It indicates the accounting update intervals.

CAR generates a few more attributes upon sucessfull authentication. These attributes are described in Table 9-2.

Table 9-2 Additional Attributes in ASN GW-CAR Flow

Attribute	Description
HA-IP-MIP4	The IP address of the HA allocated for the incoming request.
MN-HA-MIP4-KEY	The MN-HA key is used for MIP4 procedures.

Table 9-2 Additional Attributes in ASN GW-CAR Flow

Attribute	Description
MN-HA-MIP4-SPI	The SPI associated with the MN-HA-MIP4-KEY.
FA-RK-KEY	The FA-RK key will be used at ASN GW to derive MN-FA for MIP4 procedures.

Note A policy engine can parse the NAI decoration and conclude the type of authentication method for the incoming access-request for passing on to WiMAX service.

Interaction Between ASN GW and Cisco Access Registrar Through HA

After CAR returns the Access-Accept to the ASN GW, the mobile node, which initially sent the request, sends a registration request to the ASN GW. The ASN GW receives this request and sends an Access-Request to the HA. A Query-Request will be sent to the CAR by HA to receive the security context for authenticating the FA.

CAR identifies the request as HA query request, if:

- the WiMAX mobility attribute is present
- the NAS-Port-Type attribute is absent

CAR checks for a valid session in the session cache based on NAI and sends an Access-Accept to the HA.

Table 9-3 Cached Attributes

Attribute	Description
Pseudo Identity	As received from the MS in the NAI in the EAP-Response/Identity. The HAAA is required to correlate this to the true identity of the user.
NAS-ID/NAS-IP address	One or both of these parameters are cached by the HAAA. This is required to locate the serving NAS.
Framed-IP Address	The IP address allocated to the user session. This information is useful in identifying the session during AAA dynamic procedures.
MIP-RK, HA-RK,FA-RK, MN-HA	Mobility keys generated during network access authentication. These keys are cached and used by the network for mobility authentication.
HA-IP address	The IP address of the HA assigned to the MS.

Note CAR responds with the correct keys back to the HA based on the NAI in **User-Name** attribute. CAR returns an Access-Reject if it does not find a valid session for the NAI during the user authentication and authorization or if there are other errors.

Prepaid and Hot-Lining

CAR supports prepaid and hot-lining flows for WiMAX. These are supported by the existing mechanisms.

Configuring WiMAX in Cisco Access Registrar

A new service type named **wimax** will be used for the WiMAX feature in CAR. **aregcmd** command is used to configure WiMAX in CAR. WiMAX service contains—Session Manager (with a session-cache resource manager and HA resource manager), Query Service that is connected to the session manager configured for this service, and Prepaid Service, which are required to connect all the flows appearing in CAR for WiMAX. This service will be used as a container for the new key generation modules and the existing modules such as EAP services.

Configuring WiMAX in CAR involves configuration of:

- Resource Manager for WiMAX.
- Session Manager for WiMAX.
- Query Service for WiMAX.
- WiMAX properties.

Configuring the Resource Manager for WiMAX

You must configure the following two Resource Managers:

- HA (home-agent)
- HA Cache (session-cache)

The HA Resource Manager must contain the IP ranges covering all the HA IP addresses that are to be assigned in round-robin. You must configure the HA Cache Resource Manager to cache the mobility keys (Table 9-3).

Note The HA Resource Manager allocates the IP addresses to the HA. If you do not configure the HA Resource Manager properly, CAR will not generate some of the keys, which result in an Access-Reject by the NAS.

The following shows the sample configuration for HA:

```
[ /Radius/ResourceManagers/HA ]
Name = HA
Description =
Type = home-agent
Home-Agent-IPAddresses/
Entries 1 to 1 from 1 total entries
Current filter: <all>
209.165.200.225-209.165.200.254/
```

The following shows the sample configuration for HA Cache:

```
[ /Radius/ResourceManagers/HA-Cache ]
Name = HA-Cache
Description =
Type = session-cache
OverwriteAttributes = FALSE
QueryKey = User-Name
```

```
PendingRemovalDelay = 10
AttributesToBeCached/
        1. AAA-Session-ID
        2. HA-RK-Key
        3. HA-RK-SPI
        4. MN-HA-MIP4-Key
        5. MIP-RK
```

Note For generating RRQ-MN-HA key, we must configure MIP-RK in the AttributesToBeCached list.

Configuring the Session Manager for WiMAX

Before configuring WiMAX service, you must configure a session manager for WiMAX with a HA and session cache resource manager. The following shows an example configuration of a session manager with HA and session cache resource managers.

```
[ /Radius/SessionManagers/session-mgr-2 ]
    Name = session-mgr-2
    Description =
    IncomingScript =
    OutgoingScript =
    AllowAccountingStartToCreateSession = FALSE
    SessionTimeOut =
    PhantomSessionTimeOut =
    SessionKey =
    ResourceManagers/
        1. HA-Cache
        2. HA
```

Note If a default session manager is configured with the same key as that of the WiMAX session manager, the incoming WiMAX request will fail.

Configuring the Query Service for WiMAX

When you configure a query service for the WiMAX service in CAR, you must refer it to the WiMAX Session Manager that you created. While configuring WiMAX, you must refer the **WiMAX-Query-Service** parameter to a valid Query Service.

You must configure the Query key as the **User-Name** attribute, which contains the NAI. You must also configure the query service to return all the relevant mobility keys as described in Table 9-4.

Table 9-4 Mobility Keys

Key	Generated By	Used At
MN-HA-CMIP4	MN and HAAA	HA and MN
MN-HA-PMIP4	MN and HAAA	HA and PMIP4 client
MN-HA-CMIP6	MN and HAAA	MN and HA
FA-RK	MN and HAAA	MN and Authenticator
MN-FA	MN and Authenticator	FA and MN or PMIP4 client
HA-RK	HAAA	HA and Authenticator
FA-HA	HA and Authenticator	HA and FA

The following shows a sample configuration for a WiMAX Query Service:

```
[../haQueryService ]
Name = haQueryService
Description =
Type = radius-query
IncomingScript~ =
OutgoingScript~ =
SessionManagersToBeQueried/
1. session-mgr-2
AttributesToBeReturned/
1. HA-RK-Key
2. AAA-Session-ID
```

Note If AttributesToBeReturned is not configured, all the cached attributes will be returned.

Configuring WiMAX

When you configure the WiMAX service under **/Radius/Services**, you must set its type to **wimax** and provide the following configuration options:

```
[ //localhost/Radius/Services/wimax ]
Name = WiMAX
Description =
Type = WiMAX
IncomingScript~ =
OutgoingScript~ =
OutagePolicy~ = RejectAll
OutageScript~ =
HA-RK-Key = cisco123
HA-RK-LifeTime = 60
WiMAX-Authentication-Service = None
WiMAX-Session-Manager = None
WiMAX-Query-Service = None
WiMAX-Prepaid-Service = None
```

Table 9-5 WiMAX Service Parameters

Parameter	Description
Name	Required; inherited from the upper directory.
Description	An optional description of the service.
Type	Must be set to **wimax** for WiMAX service.
IncomingScript	Optional.
OutgoingScript	Optional.
OutagePolicy	Required; must be set to AcceptAll or Drop Packet, or defaults to RejectAll.
OutageScript	Optional.
HA-RK-Key	Used as the base key to generate random HA-RK-Key for all the HAs that are configured in CAR. By default, the value is `cisco123`. You can change this value.

Table 9-5 WiMAX Service Parameters (continued)

Parameter	Description
HA-RK-LifeTime	Used as time (in minutes) to regenerate the HA-RK-Keys based on its lifetime.
WiMAX-Authentication-Service	A valid eap service which can be used for WiMAX authentication. By default, this value is `none`.
WiMAX-Session-Manager	A valid session manager which has HA and HA Cache as resource managers. By default, this value is `none`.
WiMAX-Query-Service	A valid RADIUS query service configured with WiMAX session manager. By default, this value is `none`.
WiMAX-Prepaid-Service	A valid prepaid service can be given to carry out the prepaid functionality of WiMAX. Otherwise this value is set to `none`.